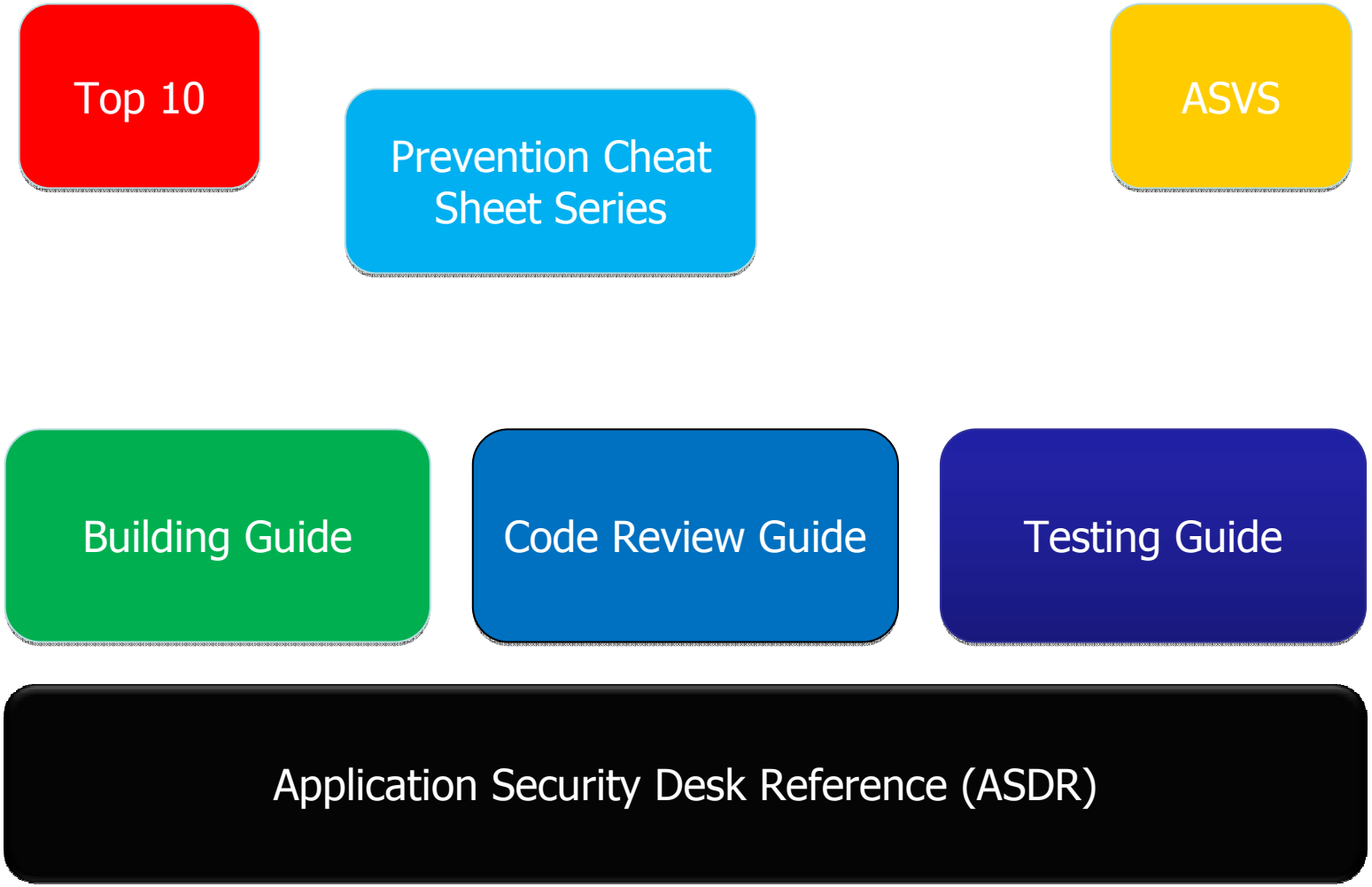
Getting Started with OWASP

The Top 10, ASVS, and the Guides

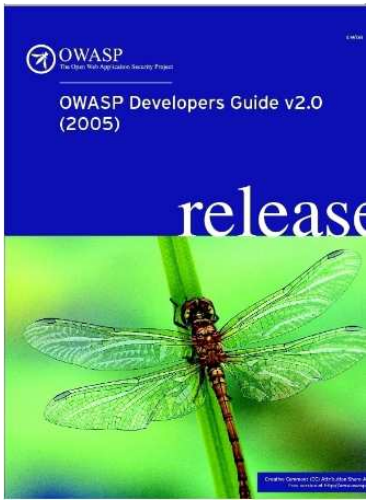
Dave Wichers
COO, Aspect Security
OWASP Board Member
OWASP Top 10 and
ASVS Projects Lead
OWASP Conferences Chair
dave.wichers@aspectsecurity.com
dave.wichers@owasp.org

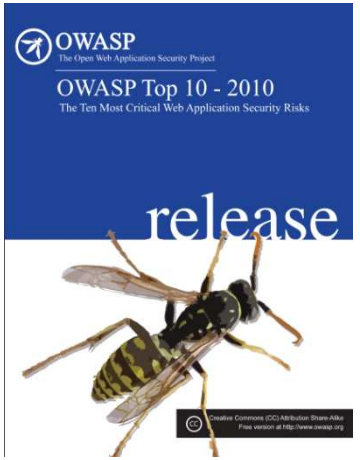
The OWASP Foundation
http://www.owasp.org/

The OWASP Documentation Projects

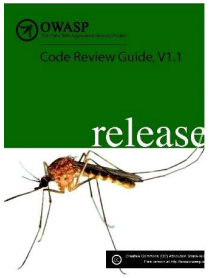


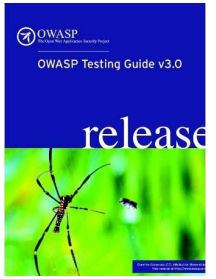
Managing Application Security Risk Using OWASP Resources





- Understand Risks
  - OWASP Top 10
- Avoiding Risks
  - OWASP Prevention Cheat Sheet Series
  - OWASP Developer's Guide
  - OWASP Enterprise Security API Project
- Measuring Risk
  - OWASP Application Security Verification Standard
  - OWASP Code Review Guide
  - OWASP Testing Guide
- Managing Risk
  - OWASP Software Assurance Maturity Model





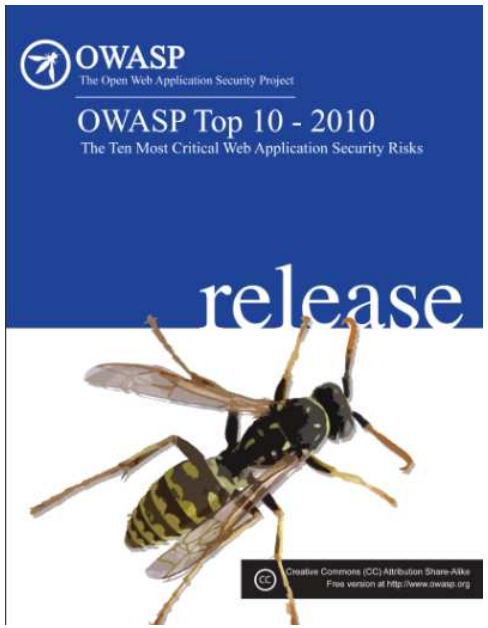
OWASP Top 10

- Purpose

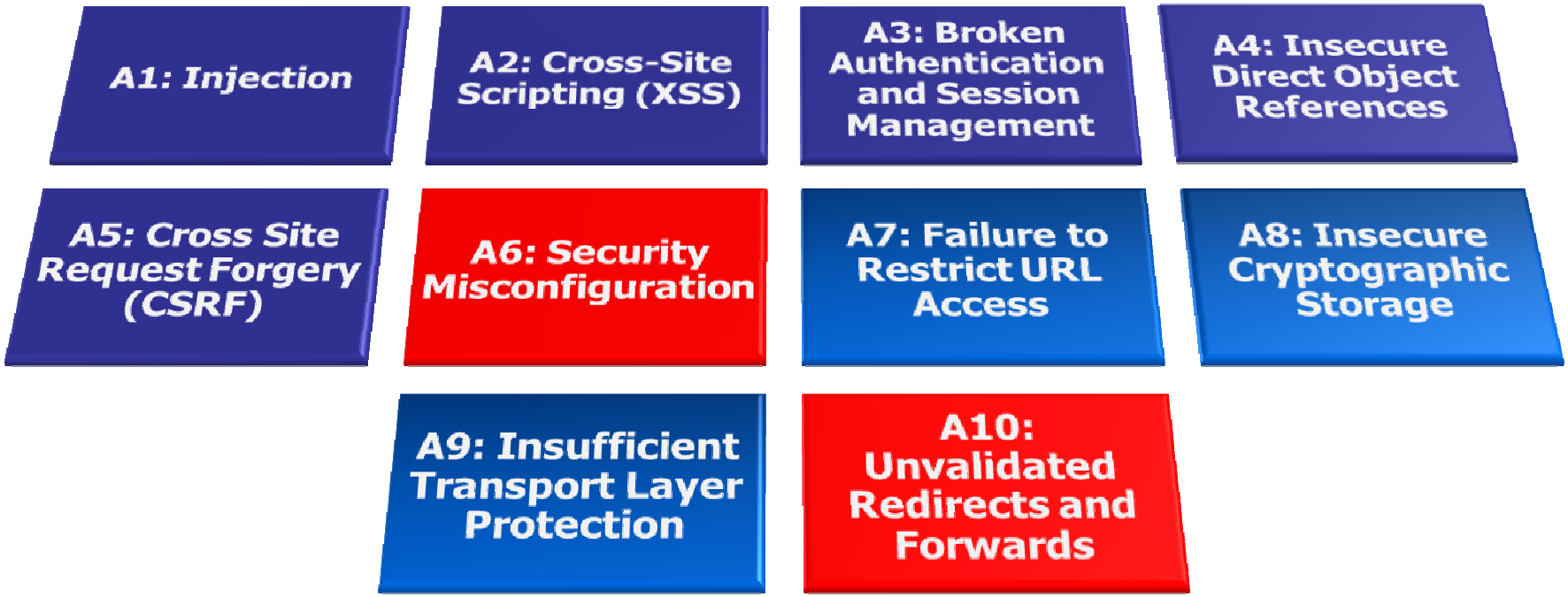
  "Educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security vulnerabilities."

- History
  - First version in 2003
  - Updated in 2004, 2007, 2010

- 24 Pages



OWASP Top 10 (2010 Edition)



OWASP
The Open Web Application Security Project
http://www.owasp.org

http://www.owasp.org/index.php/Top_10

What's Changed from 2007?

It's About Risks, Not Just Vulnerabilities

- New title is: "The Top 10 Most Critical Web Application Security Risks"

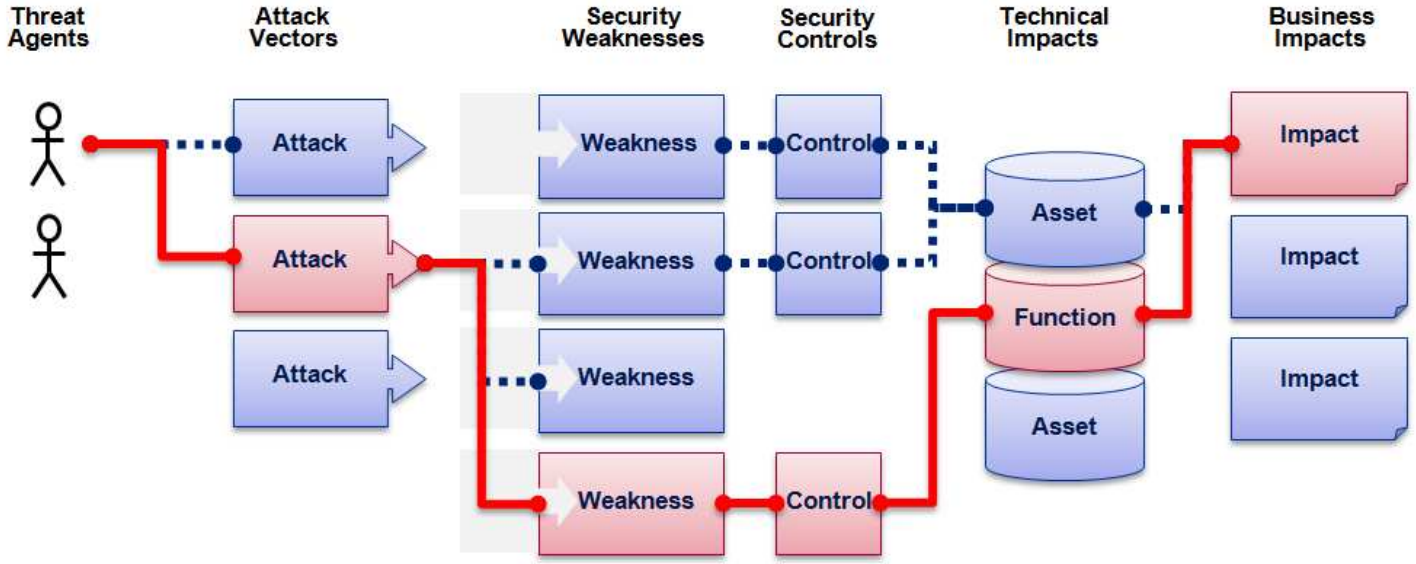
OWASP Top 10 Risk Rating Methodology

- Based on the OWASP Risk Rating Methodology, used to prioritize Top 10

2 Risks Added, 2 Dropped

- **Added: A6 – Security Misconfiguration**
  - Was A10 in 2004 Top 10: Insecure Configuration Management
- **Added: A10 – Unvalidated Redirects and Forwards**
  - Relatively common and VERY dangerous flaw that is not well known
- **Removed: A3 – Malicious File Execution**
  - Primarily a PHP flaw that is dropping in prevalence
- **Removed: A6 – Information Leakage and Improper Error Handling**
  - A very prevalent flaw, that does not introduce much risk (normally)

OWASP Top 10 Risk Rating Methodology



Threat Agent	Attack Vector	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
	1 Easy	Widespread	Easy	Severe	
?	2 Average	Common	Average	Moderate	?
	3 Difficult	Uncommon	Difficult	Minor	
	1	2	2	1	
		1.66	*	1	

Injection Example

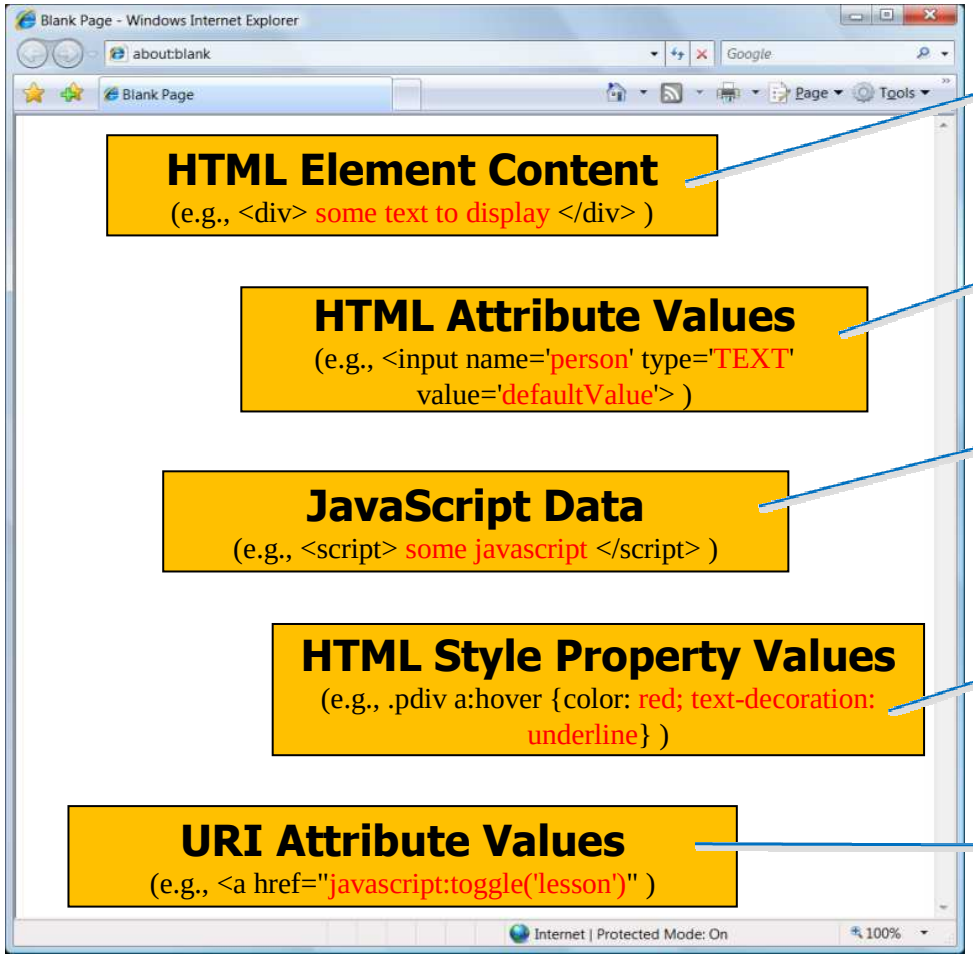
1.66 weighted risk rating

OWASP Prevention Cheat Sheet Series

How to avoid the most common web security problems

- XSS Prevention Cheat Sheet
  - www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
- SQL Injection Prevention Cheat Sheet
  - http://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
- CSRF Prevention Cheat Sheet
  - http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet
- Transport Layer Protection Cheat Sheet
  - http://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
- Cryptographic Storage Cheat Sheet
  - http://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet
- Authentication Cheat Sheet
  - http://www.owasp.org/index.php/Authentication_Cheat_Sheet

XSS Prevention Cheat Sheet



#1: &, <, >, " → &entity; ', / → &#xHH;

#2: All non-alphanumeric > 256 → &#xHH

#3: All non-alphanumeric > 256 → \xHH

#4: All non-alphanumeric > 256 → \HH

#5: All non-alphanumeric > 256 → %HH

ALL other contexts CANNOT include Untrusted Data

Recommendation: Only allow #1 and #2 and disallow all others

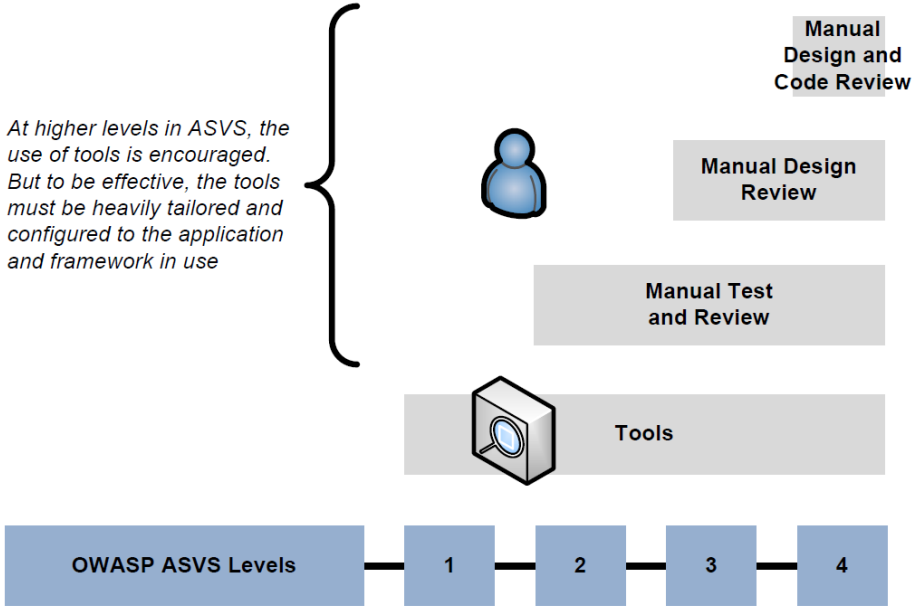
See: www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet for more details

OWASP Application Security Verification Standard (ASVS)

- OWASP's 1st Standard
  - Requires Positive Reporting!
- Defines 4 Verification Levels
  - Level 1: Automated Verification
    - Level 1A: Dynamic Scan
    - Level 1B: Source Code Scan
  - Level 2: Manual Verification
    - Level 2A: Penetration Test
    - Level 2B: Code Review
  - Level 3: Design Verification
  - Level 4: Internal Verification
- 42 Pages

What Questions Does ASVS Answer?

- How can I compare verification efforts?
- What security features should be built into the required set of security controls?
- What are reasonable increases in coverage and level of rigor when verifying the security of a web application?
- How much trust can be placed in a web application?
- Also a GREAT source of web application security requirements

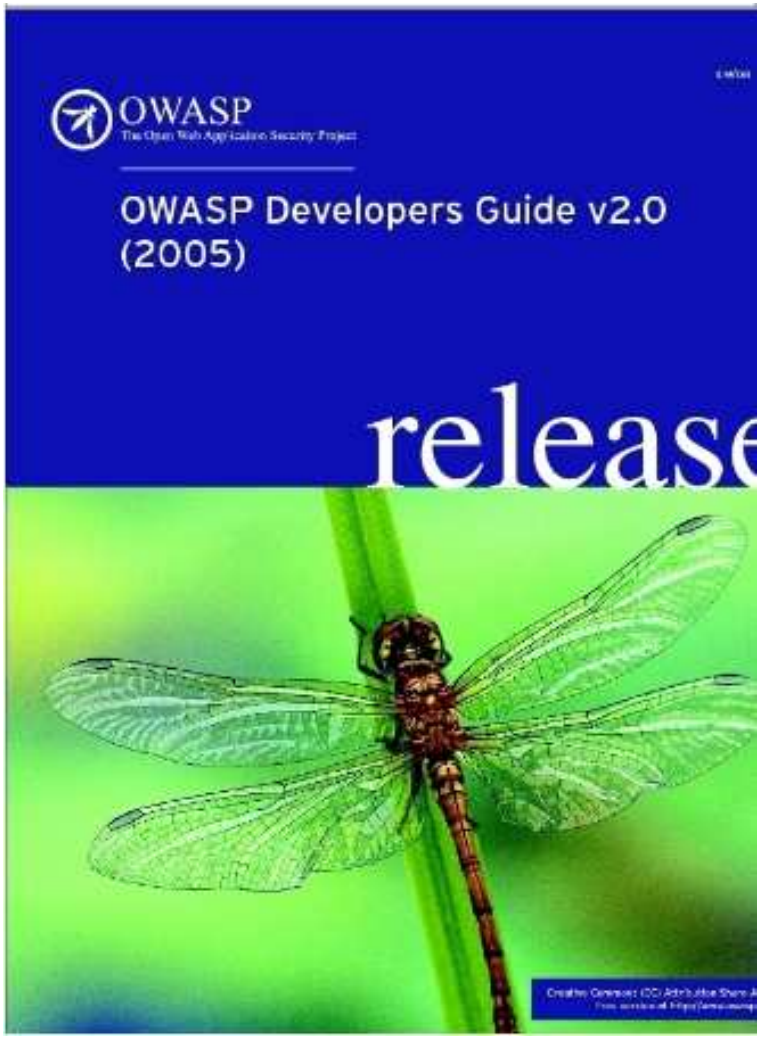


How OWASP is using the ASVS

- ASVS provides a strong structure for organizing the web application security problem space
- Using this structure to create the OWASP Common Numbering Scheme
  - http://www.owasp.org/index.php/Common_OWASP_Numbering
- Working on aligning all three guides to this common numbering scheme

OWASP Developers Guide v2.0

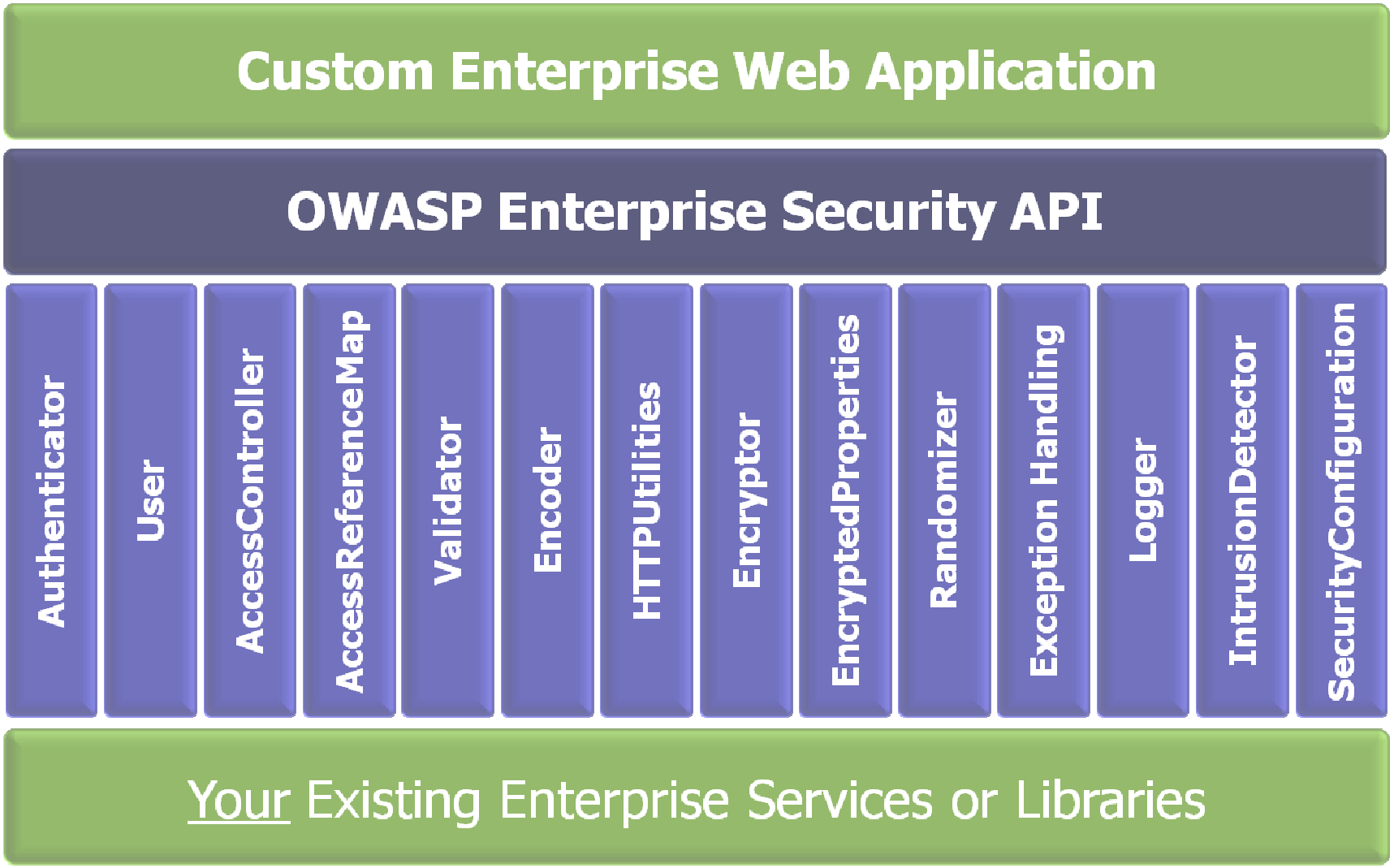
- Describes how to develop secure web applications
- Covers
  - Secure Coding
  - Threat Modeling
  - New Technologies (Web Services, AJAX)
  - 16 Security Areas
- 293 Pages



Developers Guide Past and Future

- v1.0 done in 2003, v2.0 released in 2005
- 3.0 plans
  - Align with OWASP Common Numbering / ASVS
  - Update existing sections to reflect current best practices
  - Add new sections to address new topics, including:
    - CSRF
    - Clickjacking
  - Update entire guide to cross reference relevant OWASP projects, such as ASVS, Prevention Cheat Sheets, and particularly, ESAPI.

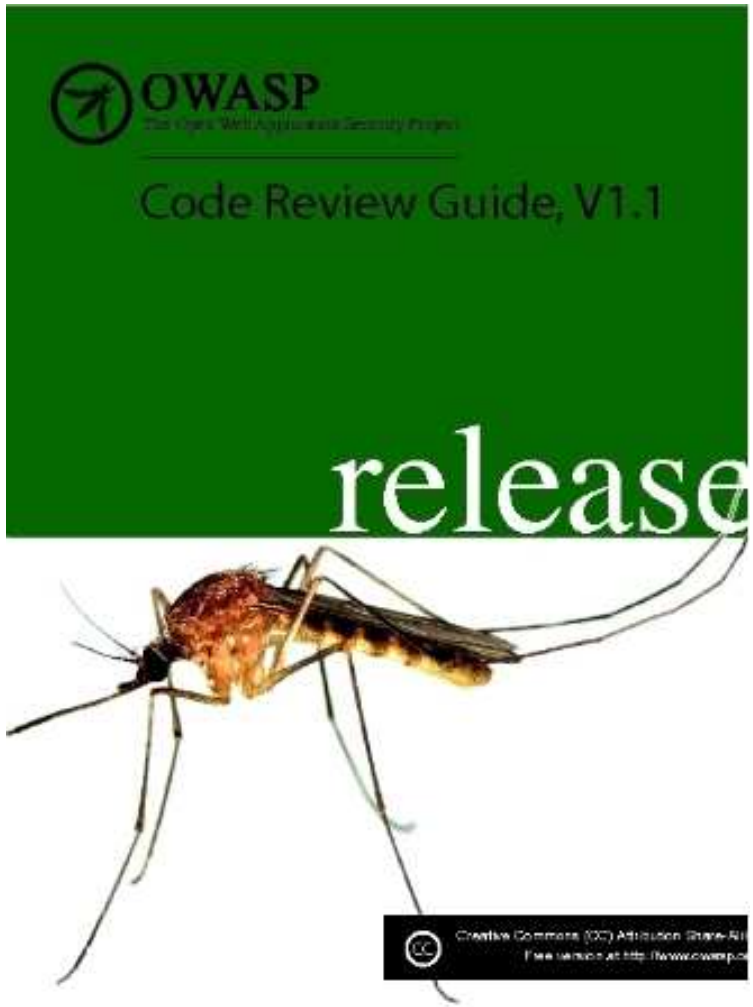
OWASP Enterprise Security API (ESAPI)



ESAPI Homepage: http://www.owasp.org/index.php/ESAPI

OWASP Code Review Guide v1.1

- World's first open source security code review guide
  - Discusses approaches to code review, reporting, metrics, risk
- Approach is "by example". (Examples of good and bad code)
  - Covers: Java, ASP, php, XML, C/C++
- By vulnerability and (more useful) by technical control
- 216 Pages

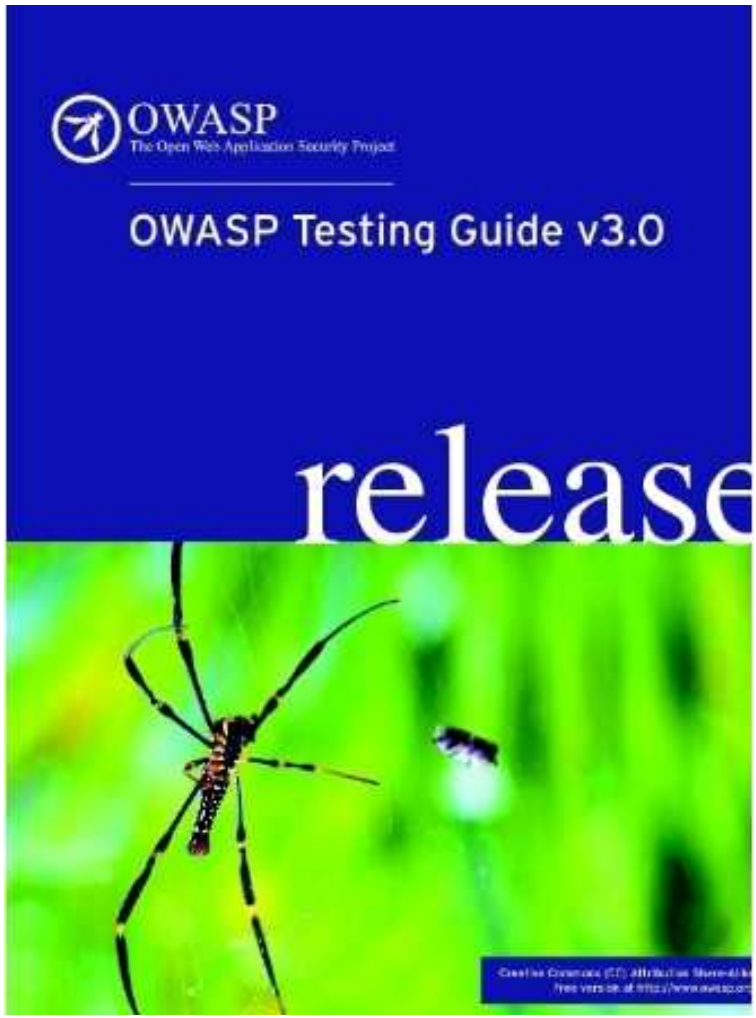


Code Review Guide Past and Future

- Version 1.1 done in 2008, 2.0 update underway
- 2.0 plans
  - Align with OWASP Common Numbering / ASVS
  - Approach to code review (Risk based approach) to be re-written
  - How to perform a code review without reviewing every line
  - Examples by Vulnerability and Technical control to be expanded and refined
  - Expand technology specific sections
  - Web Services section to be refined
  - PCI section rewritten with more x-references to other guides
  - New sections on
    - Code Analysis Tools
    - Rich Internet Applications
    - Malware and Root Kits

OWASP Testing Guide V3.0

- Massive document
  - Over 100 contributors
- OWASP Testing Approach
- Covers 10 Categories
  - 66 Specific Controls
- 347 Pages



Testing Guide Past and Future

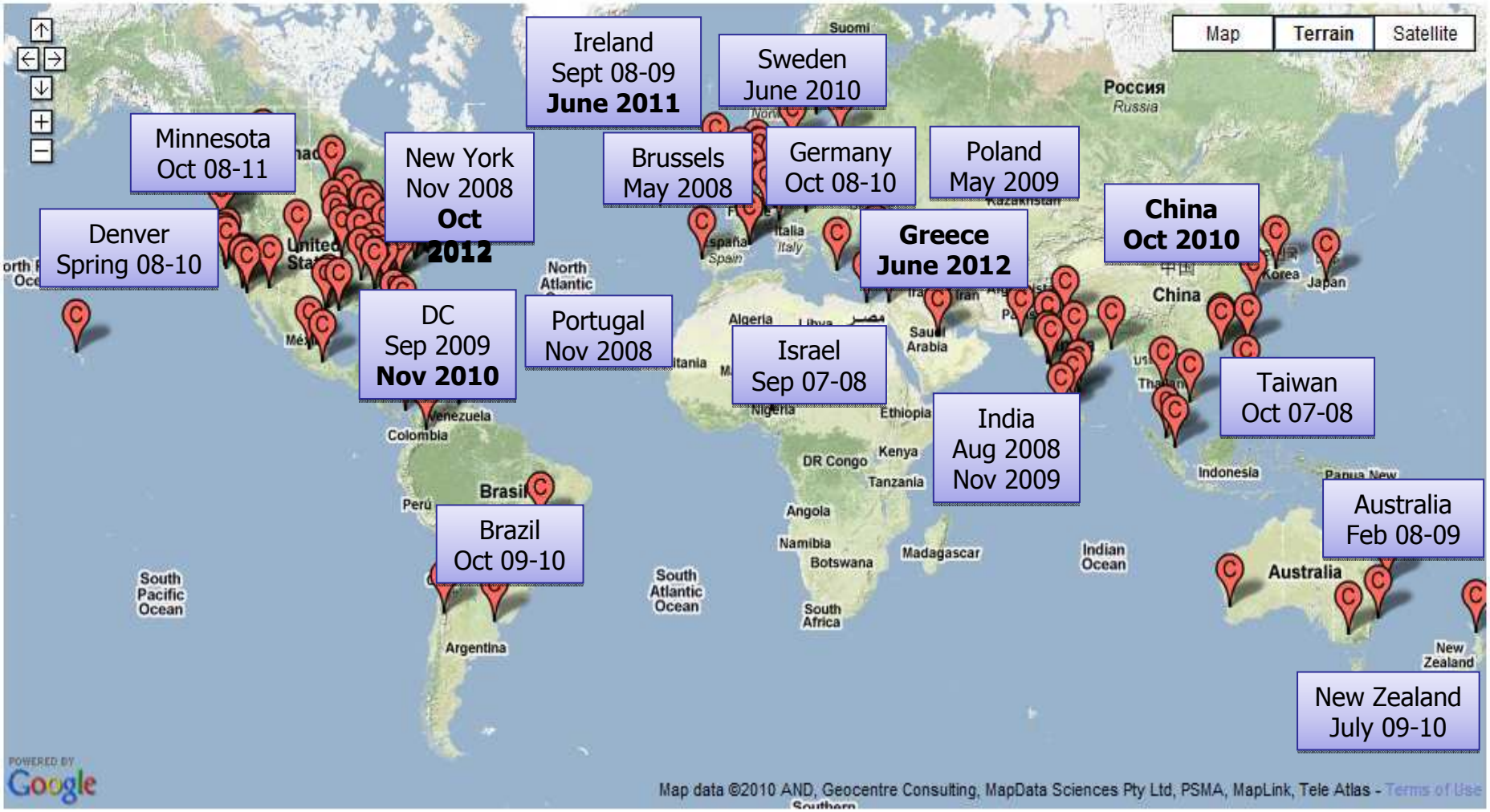
- Version 3.0 released in 2008, 4.0 update underway
  - v1.0 released in 2003, v2.0 in 2006
- 4.0 plans
  - Align with OWASP Common Numbering / ASVS
  - Review and update all existing sections
  - Eliminate some sections that aren't very useful
  - Insert new testing techniques
    - HTTP Verb tampering
    - HTTP Parameter Pollution
    - Clickjacking
  - New sections
    - Client side security
    - Firefox extensions testing

Summary: How do you address these problems?

- Develop Secure Code
  - Follow the best practices in OWASP's Guide to Building Secure Web Applications
    - http://www.owasp.org/index.php/Guide
  - Use OWASP's Application Security Verification Standard as a guide to what an application needs to be secure
    - http://www.owasp.org/index.php/ASVS
  - Use standard security components that are a fit for your organization
    - Use OWASP's ESAPI as a basis for your standard components
    - http://www.owasp.org/index.php/ESAPI
- Review Your Applications
  - Have an expert team review your applications
  - Review your applications yourselves following OWASP Guidelines
    - OWASP Code Review Guide: http://www.owasp.org/index.php/Code_Review_Guide
    - OWASP Testing Guide: http://www.owasp.org/index.php/Testing_Guide

Join, Support, and Take Advantage of the Resources Supplied by OWASP

Owasp around the world



Sampling of OWASP Conferences around the World!